

# UNITED STATES DISTRICT COURT

for the  
District of Delaware

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)

INFORMATION ASSOCIATED WITH THE GOOGLE  
ACCOUNTS "tarapet93@gmail.com" AND "lil.jenray@gmail.com"  
THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE  
LLC

Case No. 23-327M

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, incorporated herein.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 2252A(a)(1)	Transportation of Child Pornography
18 USC 2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:

See attached affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Randy Mullins

Applicant's signature

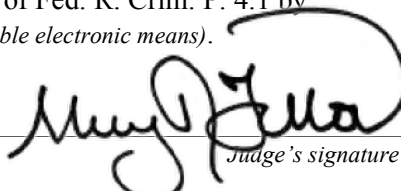
Randy Mullins, Special Agent, United States Air Force

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
\_\_\_\_\_ telephone (specify reliable electronic means).

Date: July 26, 2023

City and state: Wilmington, Delaware

  
Judge's signature

Honorable Sherry R. Fallon, U.S. Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE**

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH THE  
GOOGLE ACCOUNT  
“tarapet93@gmail.com” AND  
“lil.jenray@gmail.com” THAT IS STORED  
AT PREMISES CONTROLLED BY  
GOOGLE LLC

Case No. 23-

**AFFIDAVIT IN SUPPORT OF AN APPLICATION  
FOR A SEARCH WARRANT**

I, Randy Mullins, a Special Agent with the United States Air Force Office of Special Investigation (“OSI”), Dover, Delaware, being duly sworn, depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with Google accounts “tarapet93@gmail.com” (“TARGET ACCOUNT 1”) and “lil.jenray@gmail.com” (“TARGET ACCOUNT 2”) (together, the “TARGET ACCOUNTS”) that is stored at premises owned, maintained, controlled, or operated by Google LLC (“Google”), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Sections I of Attachment B for the accounts described in Attachment A. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in

Section II of Attachment B.

2. I am a Special Agent (“SA”) with OSI and a credentialed federal agent authorized to investigate violations of the Uniform Code of Military Justice, as well as violations of State and Federal laws where a military nexus exists. I have served with OSI since September 2016 and as a Special Agent since January 2019. I am a graduate of the Federal Law Enforcement Training Center’s Criminal Investigator Training Program, the United States Air Force Special Investigations Academy, the Sex Crimes Investigations Training Program, and the National Criminal Justice Training Center Undercover Concepts and Techniques. I graduated from the Community College of the Air Force in 2019, where I received an associate degree in Criminal Justice. Since joining OSI, I have served in multiple capacities as a Special Agent and have completed tours as a field level Special Agent, protective service officer, counterintelligence Special Agent, and have served in various supervisory roles.

3. I currently assist the Delaware Internet Crimes Against Children Task Force (the “Delaware ICAC”) with investigations where a military nexus exists. The primary goal of the Delaware ICAC will be to expand the quantity and quality of detection, investigation, apprehension, and prosecution of electronic communications-facilitated crimes against children.

4. I have experience in numerous investigative disciplines to include child exploitation, child sexual abuse, various adult sex crimes, cyber-based investigations, financial crimes, narcotics investigations, fraud, and espionage. I have received substantial training related to child exploitation, narcotics trafficking, online undercover operations, interviewing techniques, surveillance and counter-surveillance techniques, and multiple other criminal investigator-related facets.

5. As a federal agent, I am authorized to investigate violations of laws of the United States,

including Title 18, United States Code, Sections 2252A(a)(1) and 2252A(a)(5)(B), and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

6. The statements contained in this affidavit are based in part on information and reports provided by U.S. federal law enforcement agents and state law enforcement officers; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals, and my experience, training, and background as a Special Agent. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish that there is sufficient probable cause for the requested warrant.

7. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the TARGET ACCOUNTS contain evidence of violations of Title 18, United States Code, Section 2252A(a)(1) (Transportation of Child Pornography) and Title 18, United States Code, Section 2252A(a)(5)(B) (Possession of Child Pornography) (hereinafter, the “SPECIFIED FEDERAL OFFENSES”). There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

### **JURISDICTION**

8. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction

over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

**SPECIFIED FEDERAL OFFENSES**

9. As noted above, this investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections 2252A(a)(1) prohibits a person from knowingly mailing, transporting, or shipping any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer.

b. Title 18, United States Code, Sections 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

**SUMMARY CONCERNING CHILD PORNOGRAPHY, PERSONS WHO POSSESS  
AND COLLECT CHILD PORNOGRAPHY, AND HOW USE OF COMPUTERS AND  
THE INTERNET RELATES TO THE POSSESSION, RECEIPT AND/OR  
DISTRIBUTION OF CHILD PORNOGRAPHY**

10. Based on my investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who utilize the Internet to view and transport images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals, including the following:

- a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.
- b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
- d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer or cellphone, and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection, which is valued highly.
- e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, rarely destroy

correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers, cell phones and in online storage, email accounts or other online communication accounts.

f. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

11. Based on my investigative experience related to computer and internet related child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Computers, smartphones, and the internet are all methods used by child pornography collectors and those with an interest in sexual encounters with children to interact with and sexually exploit children.

b. Child pornography can be transferred via electronic mail or through file transfer protocols (“FTP”) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e. “Instant Messaging”), easy access to the internet, and online file sharing and storage, electronic devices are the preferred method of distribution and receipt of child pornographic materials.

c. The internet affords collectors of child pornography several different venues for

obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography as well as those with an interest in sexual contact with children use online resources to retrieve and store child pornography and to communicate with children, including services offered by internet portals such as AOL Inc., Yahoo!, Google, Inc., Facebook, Dropbox, Instagram, and others. The online services allow a user to set up an account with a remote computing service that provides email services, file exchange services, messaging services, as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the internet, including (for example) a smart phone. Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data.

d. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know the individuals who collect child pornography are using email accounts, online storage accounts, and other online communication accounts to obtain, store, maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

#### **RELEVANT BACKGROUND CONCERNING GOOGLE<sup>1</sup>**

12. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also

---

<sup>1</sup> The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the “Google legal policy and products” page available to registered law enforcement at [lers.google.com](https://lers.google.com); product pages on [support.google.com](https://support.google.com); or product pages on [about.google.com](https://about.google.com).



offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

13. In addition, Google offers an operating system (“OS”) for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

14. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

15. Google advertises its services as “One Account. All of Google working for you.” Once logged into a Google Account, a user can connect to Google’s full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

16. Gmail is an Internet based electronic communications system operated by Google. It permits its users to communicate using e mail through their Gmail service, instant messages, text messages, and group messages through their Hangouts and Voice services, and other social networking type methods.

17. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google

service pages, including Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

18. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

19. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

20. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

21. Google offers a cloud-based photo and video storage service called Google Photos. Users

can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

22. Google also offers a cloud storage service called Google Drive. Google Drive is automatically created for each Google Account. Users can store and upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called “Shared with me.” Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

23. Based on my training and experience, messages, emails, voicemails, photos, and videos are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation. For example, chat and photographic evidence of the distribution of child pornography may be stored in connection with the Google Account even if erased or inaccessible from the physical device.

24. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information may be evidence of who used

or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

25. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

26. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store and general Web and App Activity may reveal services used in furtherance of the crimes under investigation (e.g., social networking apps known to be frequented by those who have an interest in child pornography).

27. Therefore, Google's servers are likely to contain evidence of the crimes under investigation, as well as stored electronic communications and information concerning subscribers and their use of Google services.

### **PROBABLE CAUSE**

28. On or about May 30, 2023, OSI received a cybertip from the National Center for Missing & Exploited Children ("NCMEC"). This cybertip was initiated by Google and reported that the Google account jenray.shine@gmail.com uploaded 64 files on May 10, 2023, 28 of which Google

categorized as containing or displaying apparent child pornography. Also, in the cybertip, Google indicated that shawnnudst@gmail.com was associated with, and the backup email for jenray.shine@gmail.com account, which uploaded the child pornography.

29. Law enforcement was ultimately able to trace the file uploads to Air Force Chief Master Sergeant Paul Michael Wilcox (“Wilcox”), who was stationed at Dover Air Force Base at the time of the cybertip. Subpoena records further confirmed that both accounts in the cybertip belong to Wilcox. On June 27, 2023, a grand jury for the District of Delaware charged Wilcox with committing the SPECIFIED FEDERAL OFFENSES.<sup>2</sup> Wilcox has been ordered detained pending trial.

30. On June 15, 2023, investigators, including myself, executed a search warrant upon WILCOX’s residence and person. WILCOX also consented to an interview with your affiant that same day. During the interview, WILCOX admitted to using the shawnnudst@gmail.com account as well as the TARGET ACCOUNTS. WILCOX admitted that he saw images containing child pornography on his account, the shawnnudst@gmail.com account, but stated he could not recall how they got onto his account. He stated that someone else probably sent them to him, that he viewed them, and that they then automatically downloaded to his Google Photos. WILCOX also specifically described two images that had been part of the cybertip. WILCOX stated he deleted the photos from the shawnnudst@gmail.com account in approximately April or May 2023 after observing them in the Google Photos account because the individuals depicted in the photos were nude and appeared to be underage. He estimated approximately 25 photos were inappropriate.

31. On June 7, 2023 and June 22, 2023, your affiant obtained federal search warrants for the accounts associated with the cybertip, the jenray.shine@gmail.com and shawnnudst@gmail.com

---

<sup>2</sup> Case No. 23-cr-63-CFC.

accounts. Google has since responded to both warrants. The search warrant return for the jenray.shine@gmail.com account included the images contained in the cybertip, and your affiant confirmed the presence of child pornography. The search warrant returns for both email accounts associated with the cybertip also showed an email from May 10, 2023 indicating that the email accounts shared digital media with one another through a process called “partner sharing” using Google Photos. This email was sent shortly before the jenray.shine@gmail.com account uploaded the files containing or displaying apparent child pornography that set off the cybertip.

32. Additionally, the search warrant return for the shawnnudst@gmail.com account indicated that WILCOX shared digital media through the “partner sharing” process using Google Photos with TARGET ACCOUNT 1 in September 2020 and with TARGET ACCOUNT 2 on May 12, 2023. The shawnnudst@gmail.com shared digital media with TARGET ACCOUNT 2 two days after Google notified the shawnnudst@gmail.com account that the jenray.shine@gmail.com account was disabled for containing content involving children being sexually abused or exploited.

33. In summary, there is probable cause to believe that the TARGET ACCOUNTS contain evidence of the SPECIFIED FEDERAL OFFENSES. Specifically, WILCOX admitted to viewing images of apparent child pornography in the shawnnudst@gmail.com Google Photos with a similar description as those contained in the cybertip and ultimately located within the jenray.shine@gmail.com account. An email between the shawnnudst@gmail.com account and the jenray.shine@gmail.com account sent shortly before the jenray.shine@gmail.com account uploaded the files containing or displaying apparent child pornography indicated the shawnnudst@gmail.com account wanted to share digital media with the jenray.shine@gmail.com account through a process called “partner sharing” using Google Photos. He also shared digital media with the TARGET ACCOUNTS from the shawnnudst@gmail.com account. Specifically,

the shawnnudst@gmail.com account shared digital media through “partner sharing” using Google Photos with TARGET ACCOUNT 1 in September 2020, and with TARGET ACCOUNT 2 on May 12, 2023. Your affiant has reason to believe the digital media shared with the TARGET ACCOUNTS contains child pornography given that your affiant was able to confirm the presence of the files containing or displaying apparent child pornography that set off the cybertip within the jenray.shine@gmail.com account, and because the shawnnudst@gmail.com account requested to share photos through the “partner sharing” process shortly before the cybertip. Therefore, there is reason to believe that evidence of the SPECIFIED FEDERAL OFFENSES are present within the TARGET ACCOUNTS, which WILCOX admitted to operating during his interview on June 15, 2023.

34. Further, based on my training and experience and as described above in paragraph 11, supra, I know that individuals who collect child pornography use email accounts, online storage accounts, and other online communication accounts to obtain, store, maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices. Thus, information connected to the use of a Google account may provide direct evidence of the offenses under investigation, as well as lead to the discovery of additional evidence.

35. Information connected to the use of a Google account may also provide indirect evidence of the offenses under investigation, such as Internet searches indicative of an interest in children, or e-mails or application downloads indicating membership in forums on the dark web that are known to be dedicated to the sexual exploitation of children.

**CONCLUSION**

36. Based on the foregoing, there is probable cause for this Court to issue the requested warrant.

37. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

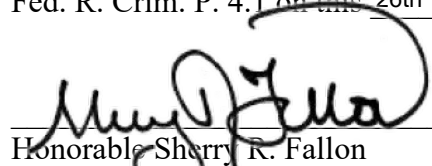
Respectfully submitted,

/s/ Randy Mullins

Special Agent Randy Mullins

Air Force Office of Special Investigations

Sworn to me over the telephone and signed by me pursuant to  
Fed. R. Crim. P. 4.1 on this 26th day of July, 2023

  
\_\_\_\_\_  
Honorable Sherry R. Fallon  
United States Magistrate Judge



**ATTACHMENT A**

**Property to be Searched**

This warrant applies to information associated with the following Google accounts (the “TARGET ACCOUNTS”), such information being stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043:

- “tarapet93@gmail.com”
- “lil.jenray@gmail.com”

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information to be disclosed by Google LLC (“Google”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any media, emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f). Air Force Office of Special Investigations submitted a preservation request on or about **June 22, 2023, reference # 36855891 for the lil.jenray@gmail.com account**. Google is required to disclose to the government for each account or identifier listed in Attachment A (“the Account”) the following information, unless otherwise indicated:

#### **A. Google Account Information**

1. All business records and subscriber information, in any form kept, pertaining to the Account, including:
  - a. Names (including subscriber names, user names, and screen names);
  - b. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
  - c. Telephone numbers, including SMS recovery and alternate sign-in numbers;
  - d. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions, including log-in IP addresses;
  - e. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers
  - f. Length of service (including start date and creation IP) and types of service utilized;

- g. Means and source of payment (including any credit card or bank account number), and detailed billing records;
- h. Change history and associated timestamps; and
- i. All cookie and user-specific advertising data, including third-party cookies.

**B. Gmail Account Information**

- 2. Gmail specific subscriber information, login and logout IP addresses and associated timestamps;
- 3. Gmail specific non-content email header information, originating message IP addresses, and account settings;
- 4. The contents of all e-mails, attachments and chat messages stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination e-mails sent, addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- 5. Contents of all available deleted emails.

**C. Google Photos and Google Drive Information**

- 6. The contents of all media associated with the account, located in but not limited to Google Photos and Google Drive, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses.

**D. Devices Associated to the Account**

- 7. All device information associated with the Account, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;
- 8. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, usernames, source and destination IP address, name of accessed Google service, and all activity logs.

**E. Google Location Information**

9. All Location History and Web & App Activity indicating the location at which the account was active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history.

**F. Browsing, Search, and Application History Information**

10. All Internet search and browsing history, and application usage history, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history.

Google is hereby ordered to disclose the above information to the government **within fourteen (14) days of issuance of this warrant. Google shall disclose responsive data, if any, by responding through the LERS portal to randy.mullins@lers.google or by sending to randy.c.mullins@leo.gov, or the Air Force Office of Special Investigations, 639 Atlantic St, Dover, Delaware, 19902, ATTN: Special Agent Randy Mullins, using UPS or another courier service, notwithstanding 18 U.S.C. 2252A or similar statute or code.**

## **II. Information to be Seized by Law Enforcement Personnel**

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of Title 18, United States Code, Section 2252A(a)(1) (Transportation of Child Pornography) and Title 18, United States Code, Section 2252A(a)(5)(B) (Possession of Child Pornography) (hereinafter, the “SPECIFIED FEDERAL OFFENSES”), including but not limited to information pertaining to the following matters:

Any and all records that relate in any way to the accounts described in Attachment A which is evidence, fruits, and instrumentalities of violations of the SPECIFIED FEDERAL OFFENSES, specifically that relate to the following:

1. Images, videos and other files depicting the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;
2. Communications or documentations regarding the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;
3. Communication or documentation regarding access to and/or interaction with minors, to include the enticement of a minor;
4. All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of the SPECIFIED FEDERAL OFFENSES under investigation;
5. Communication, information, documentation and records relating to who created, used, accessed, or communicated with the account or identifier, including records about their identities and whereabouts;
6. Evidence of the times the account or identifier listed on Attachment A was used;
7. Evidence indicating the account owner’s state of mind as it relates to the SPECIFIED FEDERAL OFFENSES under investigation;
8. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
9. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A and other associated accounts;

10. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;

11. All “address books” or other lists of contacts.